BioStar Lite

User Manual

Version V1.1

EN 102.00.BSL V1.1A

www. supremainc.com

Quality Assurance

Warranty

Suprema warrants the performance of the product specified in the specifications within the limitations set forth for a warranty period of one year from the date of delivery to the purchaser. If the purchaser claims any defects covered in this warranty in writing within the warranty period, then Suprema will repair or replace and deliver the defective product that is returned within the warranty period; provided that the purchaser shall be responsible for any transportation cost (including insurance for overseas shipping). This warranty does not apply to: (1) damage caused by strong external physical impact, overcurrent, misuse, abuse, or negligence; (2) damage to the product that has been improperly repaired, remodeled, or modified without the written permission of the provider; or (3) damage to the product that has been installed or used contrary to the manual provided by Suprema. Claims for any defects must be submitted to Suprema in writing by using the Return Material Authorization Report provided by Suprema within 30 days of the finding of the defect or within 1 year from the date of delivery. The Return Material Authorization Report must include the detailed information, model number, invoice number, and serial number of the defective product. A product without the return authorization number issued by Suprema is not considered to be eligible for the warranty. All defects must be reproducible. Excluding the above-mentioned warranties and remedies, this product is provided as-is without any expressed or implied warranties regarding product warranty, commercial viability, or availability for a particular purpose.

Disclaimer

The information in this document is provided in connection with Suprema products. No license, expressed or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document, except as provided in Suprema's Terms and Conditions of Sale for such products. Suprema assumes no liability whatso ever and Suprema disclaims any expressed or implied warranty, relating to sale and/or use of Suprema products, including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right. Suprema products are not intended for use in medical, life saving, or life sustaining applications or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should Buyer use Suprema products for any such unintended or unauthorized applications, Buyer shall indemnify and hold Suprema and its employees, head quarters, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part. Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked 'reserved' or 'undefined.' Suprema reserves these for future definitions and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Contents

Quality Assurance 2

Chapter 1

Getting Started 8

Features 8

Key Features 9

Configuration 11

BioStation T2 11

X-Station 13

Chapter 2

Using Basic Menus 15

Screen View 15

Device Management 17

Adding Devices 17

Viewing the Device Information 18

Door Management 20

Adding Doors 20

Modifying Door Information 22

Remotely Closing Doors 23

Remotely Opening Doors 23

Setting a Language 24

Viewing the Help Manual 24

Checking the BioStar Lite Firmware Version 24

Administrator Account Management 25

Adding or Modifying an Administrator Account 25

Deleting an Administrator Account 26

Logout 26

Chapter 3

Using the Home Menu 28

Screen View 28

Chapter 4

Using the User Menu 30

Screen View 30

Searching Users 31

New User Registration 32

Entering User Information 33

Registering a Card 34

Scanning a Fingerprint (Only for host devices with a fingerprint scanner) 34

User Information Modification 35

Chapter 5

Using the Log Menu..... 37

Monitoring Event Logs 37

Search Logs..... 38

Screen View 38

Search Logs 39

Chapter 6

Using the Device Menu 43

Authentication Mode Configuration..... 43

Setting Fingerprint Authentication (Only for the devices using fingerprints) 44

Setting Card Authentication 44

Setting ID Authentication 44

Setting Other Options..... 44

Setting Network 45

Setting IP Address..... 46

Setting WLAN 46

Setting Serial..... 47

Setting Display and Sound Options..... 48

Setting Time..... 49

Setting Language..... 49

Setting Background 49

Setting Theme..... 49

Setting Menu Timeout 50

Setting Popup Timeout..... 50

Setting Backlight Timeout 50

Setting Show Central Clock Display..... 50

Setting Data Format..... 50

Setting Volume..... 50

Setting Card or Fingerprint Options..... 51

Setting a Card Option..... 52

Setting a Fingerprint Option (Only for the devices using fingerprints) 52

Chapter 7

Using the Access Control Menu .. 55

Screen View 55

Holiday Group Management..... 56

Adding a Holiday..... 56

Modifying a Holiday..... 57

Deleting a Holiday 57

Timezone Management 58

Adding a Time Zone..... 58

Modifying a Time Zone 59

Deleting a Time Zone..... 60

Access Group Management..... 61

Adding an Access Group 61

Modifying an Access Group..... 62

Deleting an Access Group..... 62

Chapter 8

Using the System Profile Menu... 64

Screen View 64

System Configuration Management 65

Backup System Configuration ... 65

Restore System Configuration ... 65

User Information Management 66

Backup User Information 66

Restore User Information 66

Language Resource Management 67

Download Language Resource 67

Upload Language Resource 67

Appendix 69

Understanding the Product Details 69

Introducing Devices Supporting BioStar Lite 69

Notes for Authenticating Fingerprints on the Device 70

Authentication Mode Supported by Devices 71

Detailed Diagram 72

Device Connections 72

Door Connections 73

Troubleshooting 74

Glossary 75

Index 77

Chapter 1

Getting Started

Features

Key Features

Configuration

BioStation T2

X-Station

Getting Started

Features

- **Distributed Intelligence Access Control System**
  Suprema's distributed intelligence approach requires less hardware and less wiring than the conventional, centralized access control systems. User information, access rules, and other data can be distributed to each device to speed up authorization time and provide continual operation even when the network connection is cut off.

- **Combination of Conventional Access Control and Biometrics**
  Compared to conventional access control systems, this product was further developed to support biometric identification and access card configuration features.

- **Convenient Network Connection that Supports Both TCP/IP and RS485**
  Devices can be either connected via Ethernet or wirelessly to a local area network or directly connected via serial connections (RS485).

- **High-level Access Security Controls**
  In order to provide access control with higher level security, Suprema's access control devices incorporate state-of-the-art fingerprint recognition algorithms that won two consecutive first-place awards in the fingerprint authentication contest (FVC2004 and FVC2006).

Key Features

BioStar Lite is a system suitable for a small-sized access control environment with less than 10 devices, which provides a convenient, easy access control management to the user via a simple and intuitive UI.

- **Managing Users**

  BioStar Lite provides features for searching, adding, deleting, and modifying users according to the user information registered on the devices with an operating web-server. Any changes from adding/modifying/deleting the user will be applied to all devices on the BioStar Lite system. Please refer to '**Using the User Menu**' for details regarding managing users.

- **Managing Event Logs**

  BioStar Lite supports real-time monitoring and searching for event logs. Log monitoring and search are available on all devices on the BioStar Lite system.

- **Managing Access Group**

  BioStar Lite supports 32 holiday schedules, 128 time frames, and 128 access groups. Each time frame can be set with 5 time periods for each day of the week or 5 time periods for 2 holiday schedules selected from 32 schedules.

  Each access group consists of a total of 32 'time frames per device.

  A user in a particular access group can be authenticated within the time frame registered on a device belonging to a corresponding access group.

  Any changes from adding, modifying, or deleting access control items will be applied to all devices on the BioStar Lite system. Please refer to '**Access Group Management**' for details regarding the access group.

- **Managing Doors**

  Up to 10 doors can be remotely controlled with BioStar Lite. 2 devices can be installed in a door, which can be remotely opened or closed by the BioStar Lite. Please refer to '**Door Management**' for details regarding managing doors.

- **Managing Devices**

  The administrator can set the settings of up to 10 devices with BioStar Lite. Also, the administrator can adjust settings such as an authentication mode, communication settings, actions, screens, and sounds. All settings regarding the operating mode, display, volume, or fingerprint options modified on BioStar Lite will be applied to all devices on the BioStar Lite system. Please refer to **'Using the Device Menu'** for details regarding managing devices.

Configuration

BioStation T2

Configuration is available on devices that have a BioStar Lite server.

1 Go to the TCP/IP submenu and check 'Use BioStar Lite'.

Menu > **Network** > **TCP/IP** > **Use BioStar Lite**

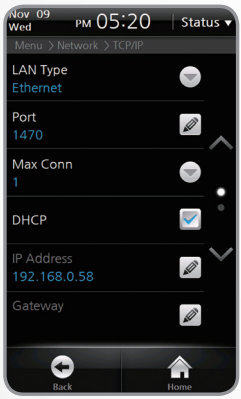


Fig1: TCP/IP submenu page 1

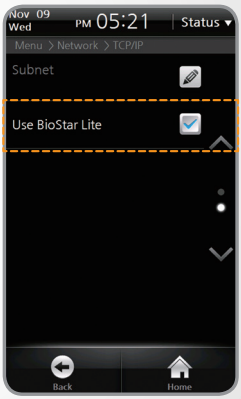


Fig2: TCP/IP submenu page 2

2 Write down the IP address currently set in the device.

Menu > **Network** > **TCP/IP** > **IP Address**

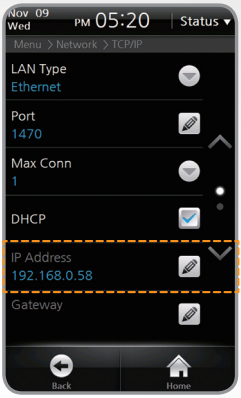


Fig. 3: TCP/IP submenu page 1

* If the IP address remains the default value of '127.0.0.1'; verify the IP configuration with your network administrator.

3 Open a web browser such as 'Internet Explorer' or 'Google Chrome' and enter the IP address of the device into the URL. The webpage for the BioStar Lite should open.

NOTE

- BioStar Lite only supports one concurrent connection.

X-Station

1 Go to the TCP/IP submenu and check 'Use BioStar Lite'.

Config > **Network** > **TCP/IP** > **Use BioStar Lite**

Fig. 1: TCP/IP submenu page 1

Fig. 2: TCP/IP submenu page 2

2 Write down the IP address currently set in the device.

Config > **Network** > **TCP/IP** > **IP Address**

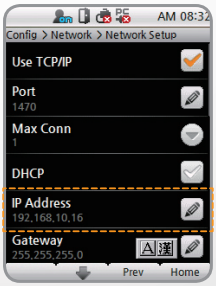


Fig. 3: TCP/IP submenu page 1

* If the IP address remains the default value of '127.0.0.1'; verify the IP configuration with your network administrator.

3 Open a web browser such as 'Internet Explorer' or 'Google Chrome' and enter the IP address of the device into the URL. The webpage for the BioStar Lite should open.

NOTE

- BioStar Lite only supports one concurrent connection.

Chapter 2

Using Basic Menus

Screen View

Device Management

Adding Devices

Viewing the Device Information

Door Management

Adding Doors

Modifying Door Information

Remotely Closing Doors

Remotely Opening Doors

Setting a Language

Viewing the Help Manual

Checking the BioStar Lite Firmware Version

Administrator Account Management

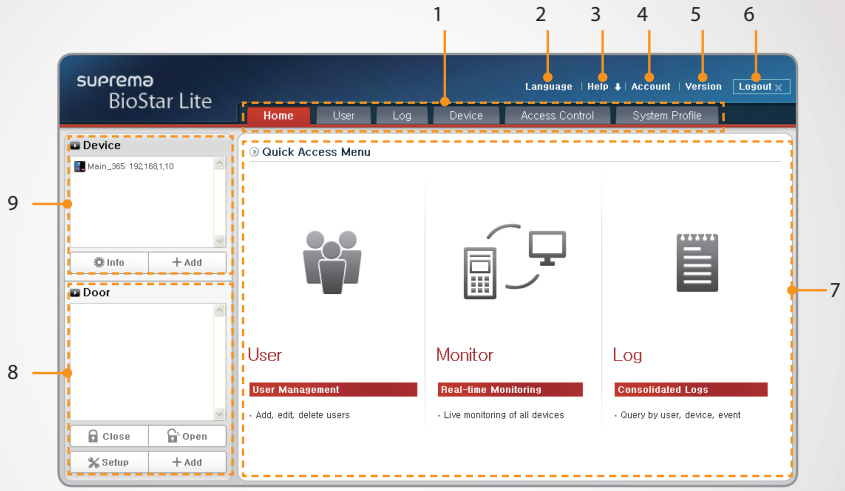
Adding or Modifying an Administrator Account

Deleting an Administrator Account

Logout

Using Basic Menus

Screen View



1 **Main Menu Tabs**: Navigate to the desired menu by clicking on the respective tab.

- **Home**: Accesses the Main Menu.
- **User**: Accesses the User Menu.
- **Log**: Accesses the Log Menu.
- **Device**: Accesses the Device Menu.
- **Access Control**: Accesses the Access Control Menu.
- **System Profile**: Accesses the System Profile Menu.

2 **Language Button**: Selects BioStar Lite's displayed language.

3 **Help Button**: Opens a help screen for the relevant menu.

4 **Account Button**: BioStar Lite administrator management.

5 **Version Button**: Displays BioStar Lite's software version.

6 **Logout Button**: Logs out of BioStar Lite. An administrator account must be created for the feature to work.

7 **Main Window**: The main contents of each menu will be displayed here.

8 **Door Management**

- **Close**: Close the selected door.
- **Open**: Open the selected door.
- **Setup**: Modify the settings of the selected door.
- **Add**: Add a new door to BioStar Lite.

9 **Device Management**

- **Info**: View detailed information of a selected device.
- **Add**: Search and add a desired device to BioStar Lite.

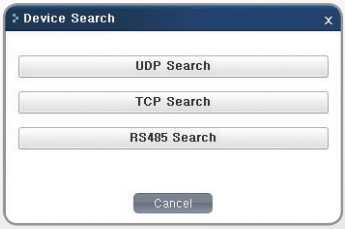
Device Management

The device tree shows all devices connected to BioStar Lite. Static IP addresses are recommended.

Adding Devices

1 Click **Add**. The Device Search window will be displayed.

2 Select a desired search method.



- **UDP Search**: Displays all devices available on the same network.
- **TCP Search**: Searches devices by entering the IP address and port.
- **RS485 Search**: Searches devices connected via RS485.

3 From the list of devices found, check the desired device(s).

4 Click **OK**. The selected device will be displayed on the list.

5 Click the red icon that appears beside the registered device(s) to synchronize the device.

NOTE

- Users, device settings and access groups will all be synchronized during the synchronization process.
- A maximum of 9 sub-devices can be registered into the BioStar Lite.

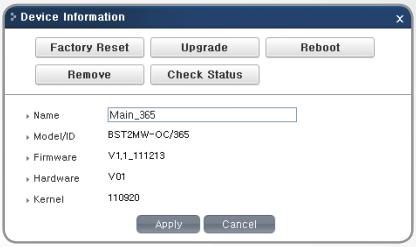
Viewing the Device Information

1 Select a device from the device tree.
The selected device will be displayed in blue.

See **'Device Connections (Page 72)'** for more details.

2 Click **Info** to view the detailed device information.

3 Click on a desired function: **Factory Reset**, **Upgrade**, **Reboot**, **Remove**, or **Check Status**.



- **Factory Reset:** Initializes the device to its factory defaults. User and log data will not be affected.
- **Upgrade**: Upgrades the firmware of the selected device.
  i. Click **Upgrade**.
  ii. Click **Browse** and select the desired firmware.
  iii. Click **Apply** to upgrade to the selected firmware.
  Click **Cancel** to cancel upgrade.
- **Reboot**: Reboots the device.
- **Remove:** Removes the selected device from the device list.
- **Check Status**: Tests the network connection to the device.

4 The device name can be modified.

5 Click **Apply** to save any changes.
Click **Cancel** to close the pop-up window.

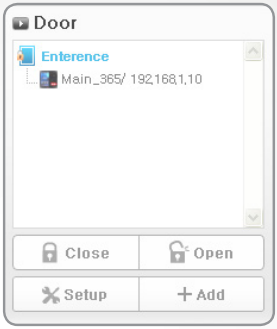
NOTE

- Click **X** on the top right corner in order to close the pop-up window.

Door Management

The door management tree shows all doors configured on BioStar Lite.

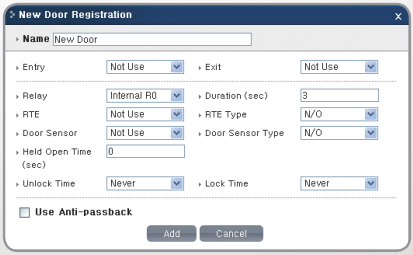
See **'Door Connections (Page 73)'** for more details.



Adding Doors

1 Click **Add**. The New Door Registration window will be displayed.

2 Enter a desired door name.



3 Configure the door.

- **Entry**: Sets the device to control entry into the room/building.
- **Exit**: Sets the device to control exit from a room/building.
- **Relay**: Sets a door relay.
- **Duration (sec)**: Sets a duration (sec) for the door to be held open. After the period, the relay will become deactivated.
- **RTE**: Sets an input trigger to open the door.
- **RTE Type**: Sets an input type to be used for the RTE (Request to Exit). (N/C: Normally Closed or N/O: Normally Open)
- **Door Sensor**: Sets a sensor input that detects the door status.
- **Door Sensor Type**: Sets an input type to be used for the door sensor. (N/C: Normally Closed or N/O: Normally Open)
- **Held Open Time (sec)**: Sets a duration (sec) a door must remain open for an alarm to trigger.
- **Unlock Time**: Sets a scheduled time when the door will remain unlocked.
- **Lock Time**: Sets the schedule when the door will remain locked.
- **Use Anti-passback**: Enables or disables the APB (anti-passback) feature.

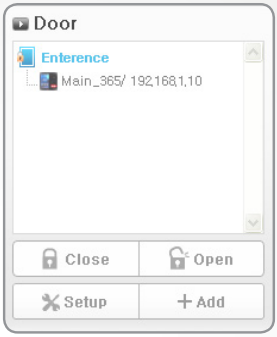
4 Click **Add** to register the new door in the door list.
Click **Cancel** to close the window.

NOTE

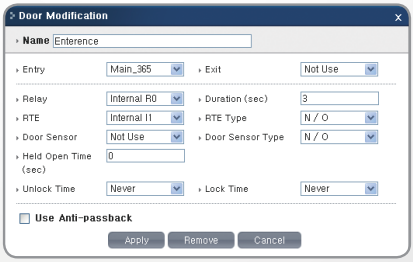
- A red icon appears after a door is initially added. Click the red icon to synchronize the settings for the added device with the user's information.
- APB (anti-passback) is a feature to limit the access of users with no entrance or departure record. Therefore, this feature distinguishes 'IN Devices' and 'OUT Devices' and allows only users authenticated on the 'IN Device' to be authenticated on the 'OUT Device' and vice versa.
- The APB (anti-passback) feature can be set only if a device is installed on both the inside and outside of the door.

Modifying Door Information

1 Select the desired door from the door list.
The selected door will be displayed in blue.



2 Click **Setup**. The door modification window will be displayed.



3 Update the desired fields.

- See **'Adding Doors (Page 20)'** for more details.

4 Click **Apply** to update the door information.
Click **Remove** to remove the selected door from the door list.
Click **Cancel** to close the window.

Remotely Closing Doors

1 Select a desired door from the door list.

2 Click **Close** to close the selected door.

Remotely Opening Doors

1 Select a desired door from the door list.

2 Click **Open** to open the selected door.

NOTE

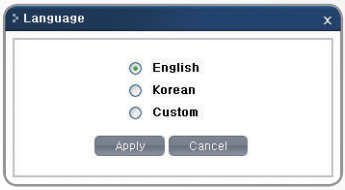
- A door that was manually opened will remain opened until it is manually closed.

Setting a Language

You can set a language to be displayed on the BioStar Lite screen.

1 Click **Language**. A language selection window will be displayed.

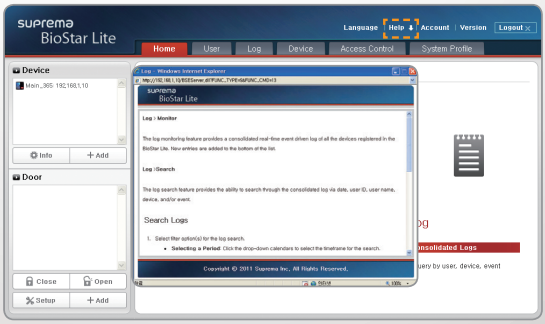
2 Select **English**, **Korean**, or **Custom**.



3 Click **Apply** to use the selected language on the displayed screen.
Click **Cancel** to cancel setting a language.

Viewing the Help Manual

Online help for the current menu can be accessed by clicking **Help**.



Checking the BioStar Lite Firmware Version

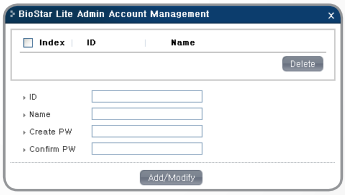
Click **Version** to see BioStar Lite's software version.

Administrator Account Management

Click **Account** to access BioStar Lite's administrator account management window.

Adding or Modifying an Administrator Account

1 Click **Account** on the top right of the screen. The BioStar Lite Admin Account Management window will be displayed.



2 Enter an administrator ID.

3 Enter the name of administrator.

4 Create a password.

5 Re-enter the password to confirm.

6 Click **Add/Modify** to register or update an administrator account.

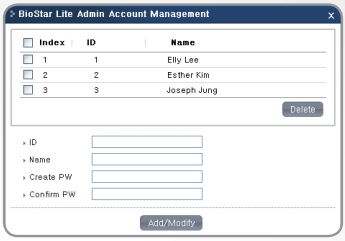
NOTE

- If the administrator account information is forgotten, the device hosting BioStar Lite can be initialized to its factory defaults. (Warning: All configurations set on BioStar Lite will be lost.)

Deleting an Administrator Account

1 Click **Account** on the top right of the screen.

The BioStar Lite Admin Account Management window will be displayed.

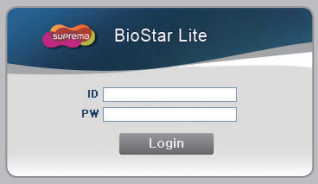


2 Check the desired account(s).

3 Click **Delete** to delete the selected accounts.

NOTE

- If no administrator account is registered on the list, BioStar Lite will automatically enter into the Home menu.
- If at least one login user is registered, a login screen is displayed when you access BioStar Lite. You return to the Home screen after the registered administrator is logged in.



- A maximum of 5 BioStar Lite administrator accounts can be created. The login ID can only include the numbers from 1 to 4294967295.

Logout

1 Click **Logout** on the top right of the screen.

NOTE

- In order to logout an BioStar Lite, administrator account must be created.

Chapter 3

Using the Home Menu

Screen View

Using the Home Menu

Screen View

1 **Home Menu Tab**: Click the tab to access the home menu.

2 **Quick Access Icons**: Click an icon to access the relevant menu.

- Add, delete, or modify a user.
- Search a user.

- View event logs of all devices in real-time.

- Search event logs by period, user, or device.

Chapter 4

Using the User Menu

Screen View

Searching Users

New User Registration

Entering User Information

Registering a Card

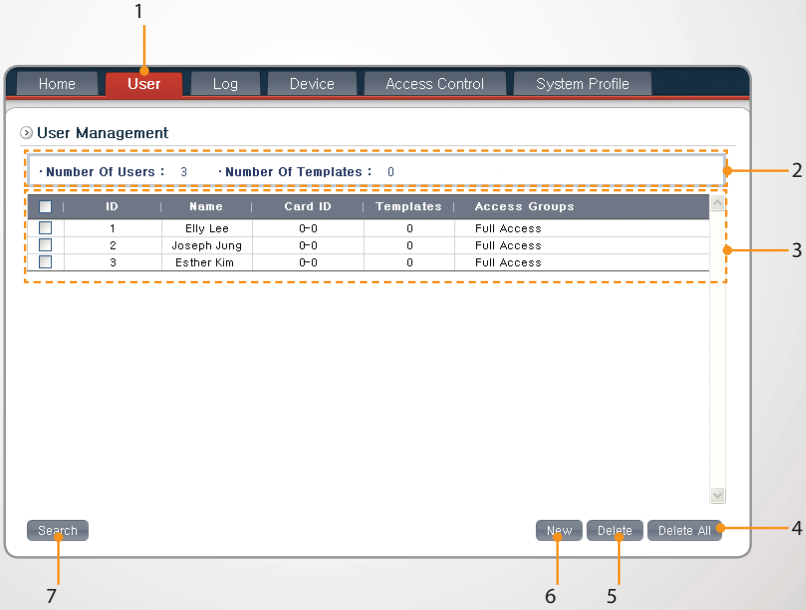
Scanning a Fingerprint
(Only for host devices with a fingerprint scanner)

User Information Modification

Using the User Menu

The user management submenu is used to add, modify, or delete users within the user database. Updates to the user database will be applied to all the devices registered into the BioStar Lite.

Screen View



1 **User Menu Tab**: Click the tab to access the user management menu.

2 **Information Window**: Displays the total number of registered users and fingerprints.

3 **User List**: Displays a list of registered users and their relevant information.

4 **Delete All Button**: Deletes all registered users from the system.

5 **Delete Button**: Deletes the selected users from the system.

6 **New User Registration Button**: Register a new user on the system.

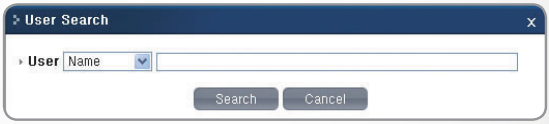
7 **Search Button**: Search for registered users on the system.

> **NOTE**
>
> - Click ID or Name to sort the users respectively.
> - You can view or modify the user's general information by clicking a user from the user list.

Searching Users

1 Click **Search**. The User Search window will be displayed.

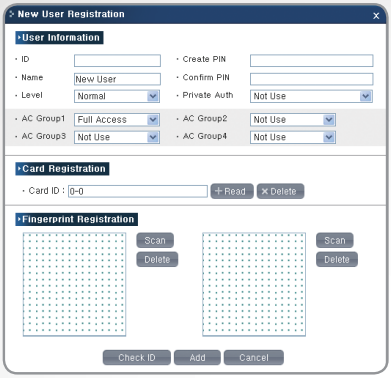
2 Select a name or ID from the user drop-down menu.



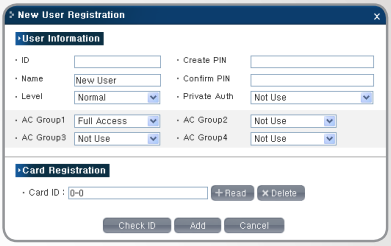
3 Enter a the respective name or ID.

4 Click **Search** to display the search results.
Click **Cancel** to close the window.

New User Registration



Window for host devices with a fingerprint scanner



Window for host devices without a fingerprint scanner

1 Click **New** to begin registration.

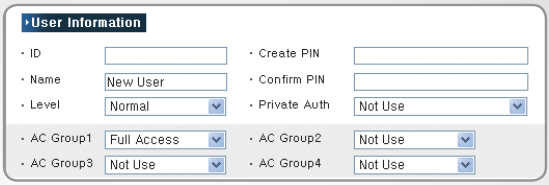
2 Enter the user information.

3 Register a card. (This step can be skipped.)

4 Scan a fingerprint. (This step can be skipped and will not be available on host device with no fingerprint scanner.)

5 Click **Add** to register the new user.
Click **Cancel** to cancel registration.

Entering User Information



1 Enter a numerical ID.

2 Click **Check ID** to check for ID availability.

3 Enter a name.

4 Enter the desired PIN number.

5 Re-enter the PIN number to confirm.

6 Set a desired user level to **Normal** or **Admin**.

7 Set a private authentication mode. This mode will be prioritized over the device's default settings. See **'Authentication Mode Configuration (Page 43)'** for more details.

8 Set an access group for the user.
Each user can be a part of 4 different access groups.

NOTE

- A user in a particular access group can be authenticated within the time frame set on a device belonging to a corresponding access group. See **'Using the Access Control Menu (Page 54)'** for more details.

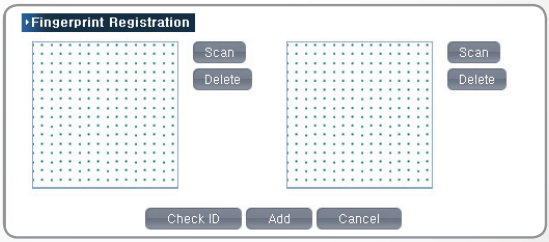
Registering a Card

1 Click **Read** to register a card.

2 Follow the instructions displayed on the linked device.
If the scan is successful, the card ID will be displayed on BioStar Lite.

3 Click **Delete** to delete the entered card ID.

Scanning a Fingerprint (Only for host devices with a fingerprint scanner)



1 Click **Scan** to register a fingerprint.

2 Follow the instructions displayed on the linked device.

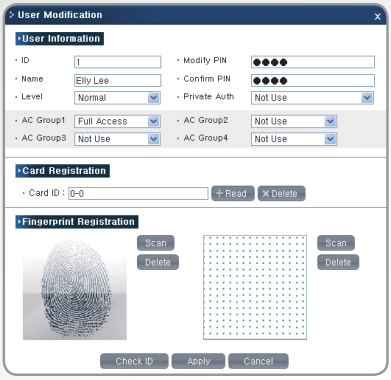
3 To register an additional fingerprint, repeat steps 1 and 2.
See **'Notes for Authenticating Fingerprints on the Device (Page 70)'** for details on how to properly register a fingerprint.

4 Click **Add** to register the scanned fingerprint.
Click **Cancel** to cancel registering the scanned fingerprint.

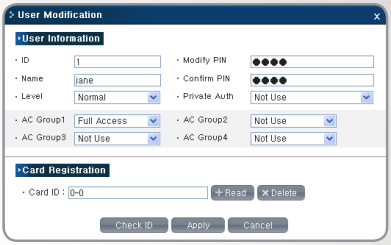
NOTE

- Upon success, an image of the fingerprint will be displayed.
- Click **Delete** next to the scanned fingerprint to delete corresponding fingerprint.

User Information Modification



Window for host devices with a fingerprint scanner



Window for host devices without a fingerprint scanner

1 Click on a desired user from the user list.

2 Update user information.

3 Update card information.

4 Update fingerprint information for the devices using fingerprints.

5 Click **Apply** to apply the change.
Click **Cancel** to cancel the change.

Chapter 5

Using the Log Menu

Monitoring Event Logs

Search Logs

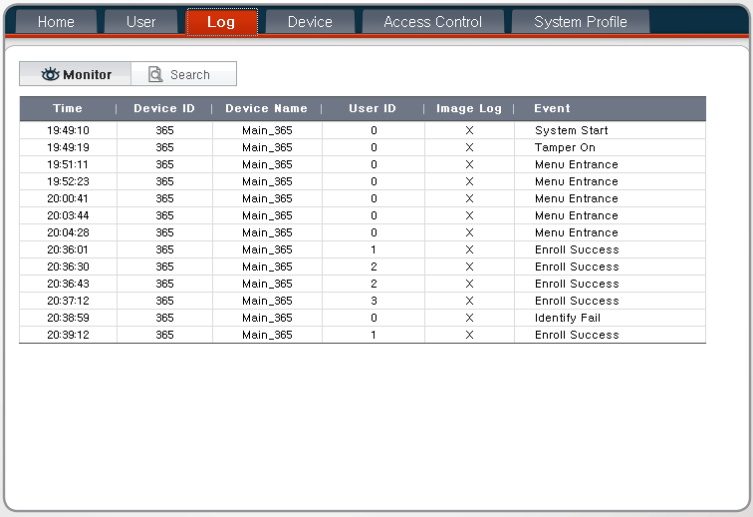
Screen View

Search Logs

Using the Log Menu

Monitoring Event Logs

The log monitoring feature provides a consolidated real-time event driven log of all the devices registered in the BioStar Lite. New entries are added to the bottom of the list. The consolidated log will display a complete list of events even from devices that do not have a BioStar Lite server.

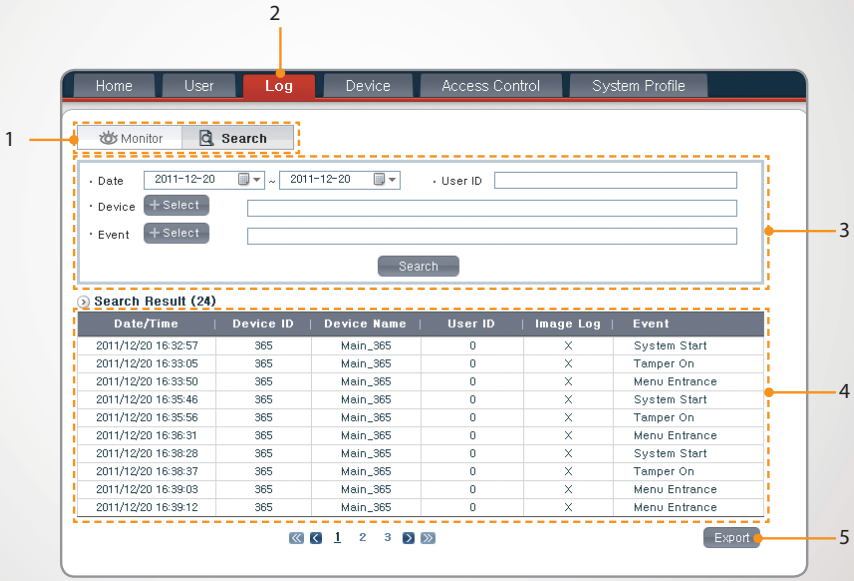


Time	Device ID	Device Name	User ID	Image Log	Event
19:49:10	365	Main_365	0	X	System Start
19:49:19	365	Main_365	0	X	Tamper On
19:51:11	365	Main_365	0	X	Menu Entrance
19:52:23	365	Main_365	0	X	Menu Entrance
20:00:41	365	Main_365	0	X	Menu Entrance
20:03:44	365	Main_365	0	X	Menu Entrance
20:04:28	365	Main_365	0	X	Menu Entrance
20:36:01	365	Main_365	1	X	Enroll Success
20:36:30	365	Main_365	2	X	Enroll Success
20:36:43	365	Main_365	2	X	Enroll Success
20:37:12	365	Main_365	3	X	Enroll Success
20:38:59	365	Main_365	0	X	Identify Fail
20:39:12	365	Main_365	1	X	Enroll Success

Search Logs

The log search feature provides the ability to search through the consolidated log via date, user ID, user name, device, and/or event.

Screen View



1 **Mode**: Click **Monitor** to access the real-time monitoring window and **Search** to access the search window.

2 **Log Menu Tab**: Click the tab to access the log menu.

3 **Search Parameters**

- **Date**: Designate a time periods for the search.
- **User ID**: Enter the desired user ID(s). A blank entry will search all user IDs.
- **Device Search**: Enter the desired device(s). A blank entry will search all devices.
- **Event Search**: Select the desired event(s). A blank entry will search all events.
- **Search Button**: Click **Search** to begin the search.

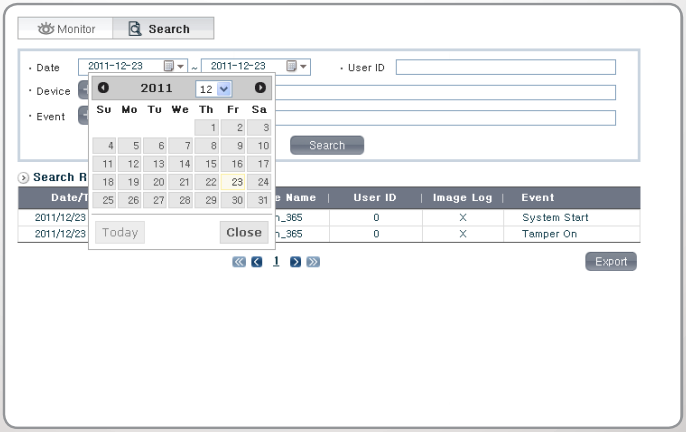
4 **Search Results Window**: Displays the search results.

5 **Export Button**: Save the event logs in a CSV file format.

Search Logs

1 Input the desired search parameters.

- **Selecting a Period:** Click the drop-down calendars to select the timeframe for the search.

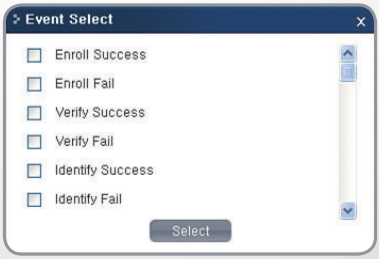


- **Selecting a Device**
  i. Click **Select** to display the connected device in a pop-up window.

  ii. Select a device(s) to search.
  iii. Click **Select** to add the devices to the device list.

- **Entering a User ID**: Enter either the ID or name of the user.
  Multiple IDs can be entered by separating each with semicolons (;) as seperators.

- **Selecting an Event**
  i. Click **Select** to display events.
  ii. Select an event(s) to search.



  iii. Click **Select** to add the events to the event list.

2 Click **Search** to display the search results.
The search results may span across several pages.

3 Click **Export**, and then click **Download** in a pop-up window in order to designate a location to save a file in. Event logs will be saved as a file on the designated path.

NOTE

- When exported as a file, the file is saved in the CSV format (',' separator; 'dat' extension). This file can be modified with a text editor or MS Excel.
- The exported file is stored in UTF-8 encoding.
- When using MS Excel, MS Excel must be running prior to opening the exported file via the file open menu.
- If an export file is not downloaded, click the right mouse button and then press '**Save as**'.

Chapter 6

Using the Device Menu

Authentication Mode Configuration

Setting Fingerprint Authentication (Only for the devices using fingerprints)

Setting Card Authentication

Setting ID Authentication

Setting Other Options

Setting Network

Setting IP Address

Setting WLAN

Setting Serial

Setting Display and Sound Options

Setting Time

Setting Language

Setting Background

Setting Theme

Setting Menu Timeout

Setting Popup Timeout

Setting Backlight Timeout

Setting Show Central Clock Display

Setting Data Format

Setting Volume

Setting Card or Fingerprint Options

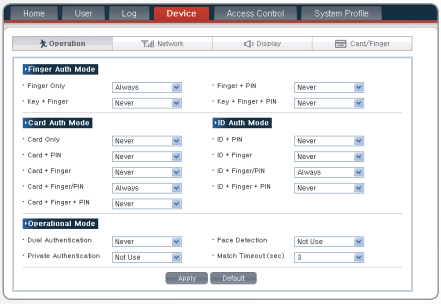
Setting a Card Option

Setting a Fingerprint Option (Only for the devices using fingerprints)

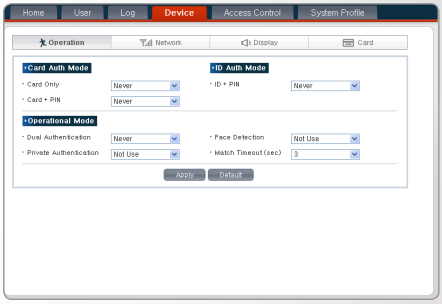
Using the Device Menu

Authentication Mode Configuration

The device operation submenu is used to configure the authentication modes and matching timeout duration. Any modifications will be applied to all the devices connected to the BioStar Lite and having inner web servers. If the device does not have the option, it will default to the closest possible option.



Window for host devices with a fingerprint scanner



Window for host devices without a fingerprint scanner

1. Select the desired activation period for each ID authentication mode.
   Only one of each active timezone can be set per group.
2. Select if you wish to use dual authenication, private authenication, and/or face detection.
3. Select the maximum time the device should search the database before returning a result.
4. Click **Apply** to apply settings to the all the devices connected to the BioStar Lite.
   Click **Default** to reset the menu to its defaults. The changes will not be automatically applied.

Setting Fingerprint Authentication (Only for the devices using fingerprints)

- **Finger Only**: Authenticates using only a fingerprint.
- **Finger + PIN**: Authenticates using both fingerprint and password.
- **Key + Finger**: Authenticates using both a T/A key and fingerprint.
- **Key + Finger + PIN**: Authenticates using a T/A key , fingerprint, and password.

Setting Card Authentication

- **Card Only**: Authenticates using only a card.
- **Card + PIN**: Authenticates using both card and password.
- **Card + Finger**: Authenticates using both card and fingerprint.
- **Card + Finger/PIN**: Authenticates using card and either fingerprint or password.
- **Card + Finger + PIN**: Authenticates using card, fingerprint, and password.

Setting ID Authentication

- **ID + PIN**: Authenticates with using ID and password.
- **ID + Finger**: Authenticates using both ID and fingerprint.
- **ID + Finger/PIN**: Authenticates using both ID and either fingerprint or password.
- **ID + Finger + PIN**: Authenticates using ID, fingerprint, and password.

Setting Other Options

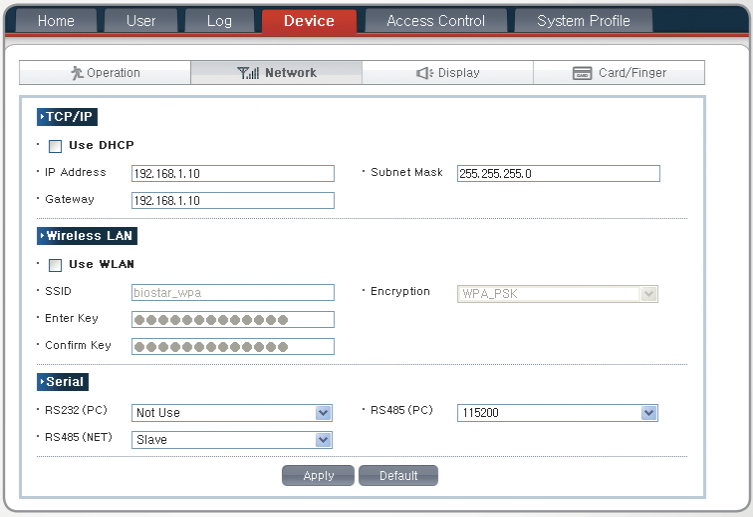
- **Dual Authentication**: Authenticates using IDs, fingerprints, or cards of two people. The entry relay operates only when two different users try authentication and the second user should try authentication within at least 15 seconds after the first user is authenticated.
- **Face Detection**: Authenticates by detecting a face after successful authentication. This is not facial recognition.
- **Private Authentication**: Authenticates by customized methods for each individual.
- **Match Timeout (sec)**: Sets a length of time (in seconds) for determining successful authentication.

NOTE

- Depending on the type of device, some authentication modes may not be supported ; the device will then, default to the closest possible mode. Refer to **'Authentication Mode Supported by Devices (Page 71)'** for details.

Setting Network

The device network submenu is used to configure the various communication and network settings. Any modifications, excluding TCP/IP, will be applied to all the devices connected to the BioStar Lite and having inner web servers. The TCP/IP settings will only affect the master device.



1 Enter the desired TCP/IP settings values for the master device.

2 Enter the desired WLAN setting values. (Only applies to WIFI devices)

3 Select the desired serial communication settings.

4 Click **Apply** to apply settings to all the devices connected to the BioStar Lite.

Click **Default** to reset any change, which will not be applied to the device.

NOTE

- Modifications to the TCP/IP settings will only affect the master device.
- The settings for serial communication will be applied to all the devices connected to the BioStar Lite and having inner web servers.
- Applicable network settings will vary from device to device.

Setting IP Address

- **When using a dynamic IP**
  i. Check **Use DHCP** to use DHCP.
  An IP address will be automatically assigned to the device.
- **When using a static IP**
  i. Uncheck **Use DHCP** to use a static IP address.
  ii. Enter the IP address, gateway, and subnet mask.

Setting WLAN

1 Check **Use WLAN** to enable the WLAN feature.

2 Set the following details when checking **Use WLAN**.

3 Enter SSID(up to 32 characters).

4 Set an encryption method (Not Use/WEP/WPA-PSK).

5 If encryption is enabled, enter an encryption key (up to 13 characters).

6 Re-enter the encryption key in the confirmation field to confirm.

NOTE

- If the WLAN is enabled, TCP/IP will be disabled.
- SSID is a unique, 32-byte identifier on each header of packets transmitted over wireless LANs, which is used as an ID for a wireless device when connected.

Setting Serial

- RS232(PC): Available when RS485 is disabled.

  Select a baud rate to enable the port.

  (Not Use/ 9600/ 19200/ 38400/57600/115200)

- RS485(PC): Select a baud rate to enable the port.

  (Not Use/ 9600/ 19200/ 38400/57600/115200)

- RS485(NET): Sets mode for devices connected via RS485.

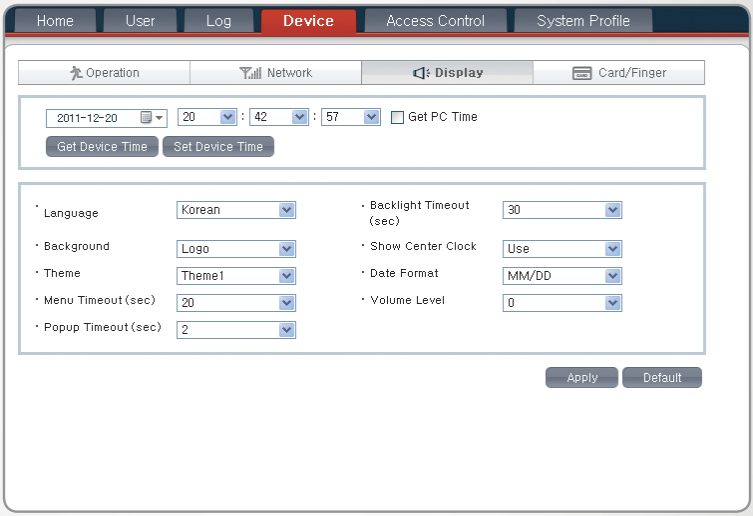
  (Not Use/ Host/ Slave)

NOTE

- The BioStation T2 can not support both RS232 and RS485 simultaneously.
- A host device can have slave devices connected via RS485.
- When you add a device through **RS485 Search**, the **RS485(NET)** must be set as **Host**.

Setting Display and Sound Options

The device display submenu is used to configure the time and various OSD settings. Any modifications will be applied to all the devices connected to the BioStar Lite and having inner web servers. The OSD settings will only affect devices with a LCD screen.



1 Set the current date and time.

2 Select the desired OSD settings.

3 Click **Apply** to apply settings to all the device connected to the BioStar Lite.
Click **Default** to reset any change, which will not be applied to the device.

Setting Time

You can check or change the time on the Device.

- **Checking Time**

  Click **Get Device Time** to check the time on the master device.

- **Changing Time**

  i. Set the date with a drop-down calendar.

  ii. Set the desired hour, minute, and second.

  iii. Click **Set Device Time** to apply the changed time.

- **Synchronizing with Host PC Time**

  i. Check the **Get PC time** checkbox.

  ii. Click **Set Device Time** to automatically synchronize the device time with the time of the host PC.

Setting Language

You can set the language to be displayed by selecting among **Korean**, **English**, or **Custom**.

Setting Background

You can set the device background to be displayed by selecting among **Logo**, **Notice**, **Slide**, or **PDF**.

Setting Theme

You can set the background theme for the device.

Theme1, **Theme2**, **Theme3**, and **Theme4** are available.

Setting Menu Timeout

You can set the amount of idle time (sec) before the menu disappears.

Always On, **10**, **20**, and **30** are available.

Setting Popup Timeout

You can set the duration (sec) before the popup window disappears.

0.5, **1**, **2**, **3**, **4**, and **5** are available.

Setting Backlight Timeout

You can set the amount of idle time (sec) before the backlight turns off.

Always On, **10**, **20**, **30**, **40**, **50**, and **60** are available.

Setting Show Central Clock Display

You can set to enable or disable the large clock in the center of the LCD.

It can be set to **Use** or **Not Use**.

Setting Data Format

You can set the format for the displayed date.

It can be set as **MM/DD** or **DD/MM**.

Setting Volume

You can set the volume output of the device.

0, **10**, **20**, **30**, **40**, **50**, **60**, **70**, **80**, **90**, and **100** are available.

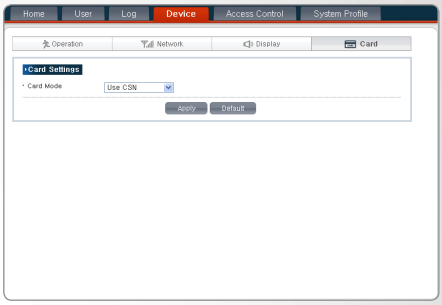
NOTE

- Applicable OSD settings will vary from device to device.
- The language setting does not change when restoring default values.

Setting Card or Fingerprint Options

The device card/finger submenu is used to configure the various scanner settings. Any modifications will be applied to all the devices connected to BioStar Lite and having inner web servers.

Window for host devices with a fingerprint scanner



Window for host devices without a fingerprint scanner

1. Select a mode for the card scanner.
2. Select various fingerprint scanner settings for devices using fingerprints.
3. Click **Apply** to apply settings to all the devices connected to the BioStar Lite.
   Click **Default** to reset any change, which will not be applied to the device.

Setting a Card Option

You can set mode for a card to be used as an access control device.

Not Use and **CSN Mode** are available.

> **NOTE**
>
> - The **CSN Mode** uses the CSN (Card Serial Number) to authenticate the user. The CSN of a scanned card will be compared with the CSN information stored within the user DB.

Setting a Fingerprint Option (Only for the devices using fingerprints)

You can adjust fingerprint authentication settings to be used as an access control device.

- **Security Level**

  You can set the verification level for fingerprint authentication.

  Normal, **Secure**, and **Most Secure** are available. **Normal** is recommended for a regular Time and Attendance. **Secure** or **Most Secure** is recommended for an environment that requires higher access control security.

- **Fast Mode**

  You can set the authentication speed for fingerprint authentication.

  Normal, **Fast**, **Fastest**, and **Auto** are available.

- **Fake Detect**

  You can set the device to enable or disable a preventive test for a fake fingerprint attack. **Use** and **Not Use** are available.

- **Scan Timeout**

  You can set amount of time (sec) to attempt a scan from 1 to 20 .

  If a user does not place a finger on the device within this period, authentication will fail.

- **Sensitivity**

  You can set the sensitivity value from 1 to 7 for the fingerprint scanner of device.

  (1- Most insensitive, 7- Most sensitive)

- **View Image**

  You can set to display or hide a fingerprint image upon a successful scan.

  Use and **Not Use** are available.

  The fingerprint image can be verified on the screen upon scanning and guide the user to correctly place the finger.

NOTE

- Increasing the security level will indirectly increase the FRR(False Reject Rate) because the stricter authentication protocols will reject more inconsistencies.
- Setting **Fast Mode** to **Auto** will set the authentication speed of the device proportional to the total number of templates registered on the device.
- When the sensitivity is set to low, the scanned fingerprint image is displayed in a higher quality. Set the sensitivity to the maximum value in a normal environment. When direct sunlight is present, set the sensitivity to low in order to minimize the effect of direct sunlight.
- Using View Image is helpful in determining if a fingerprint has been properly scanned.
- Applicable fingerprint settings will vary from device to device.

Chapter 7

Using the Access Control Menu

Screen View

Holiday Group Management

Adding a Holiday

Modifying a Holiday

Deleting a Holiday

Timezone Management

Adding a Time Zone

Modifying a Time Zone

Deleting a Time Zone

Access Group Management

Adding an Access Group

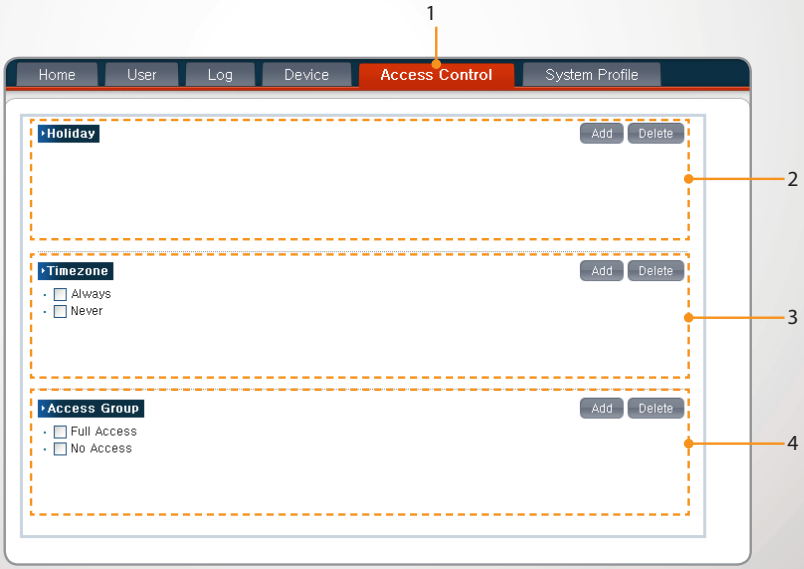
Modifying an Access Group

Deleting an Access Group

Using the Access Control Menu

BioStar Lite supports up to 128 time zones consisting of seven day schedules along with two holiday schedules. Each day in a time zone may include as many as five distinct time periods. In total, BioStar supports up to 128 access groups for which a time zone may be specified for each device.

Screen View



1 **Access Control Menu Tab**: Click the tab to access the access control menu.

2 **Holiday Window**: Add, modify or delete the registered holidays.

3 **Time Zone Window**: Add, modify or delete the registered timezones.

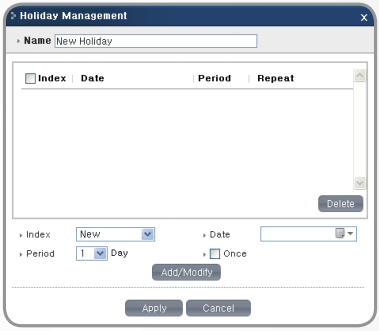
4 **Access Group Window**: Add, modify or delete the registered access groups.

Holiday Group Management

Holiday groups can be used to setup timezones and access groups.

Adding a Holiday

1 Click **Add**. The Holiday Management window will be displayed.



2 Enter a name for a holiday.

3 Select **New** in the index field.

4 Select the start date of holidays from the drop-down calendar.

5 Select the duration of holidays from the drop-down calendar.

6 Check **Once** if this is a one-time holiday.

7 Click **Apply/Modify** to add a holiday to the list.

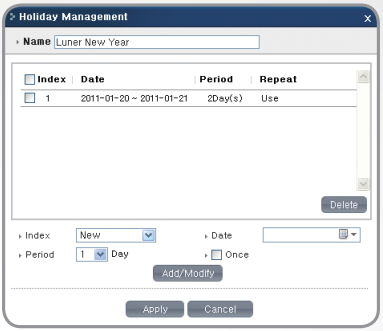
8 Click **Apply** to update the holiday list.
Click **Cancel** to close the window.

NOTE

- Up to 32 holiday schedules can be added.

Modifying a Holiday

1 Click on a holiday group from the list. A window for modifying a holiday is displayed.



2 Select a holiday number from the index field.

3 Modify the desired fields.

4 Click **Add/Modify** to update the selected holiday.

5 Click **Apply** to update the holiday list.
Click **Cancel** to cancel the update.

Deleting a Holiday

1 Select a checkbox of a desired holiday group(s).

2 Click **Delete** to remove the selected holiday groups.

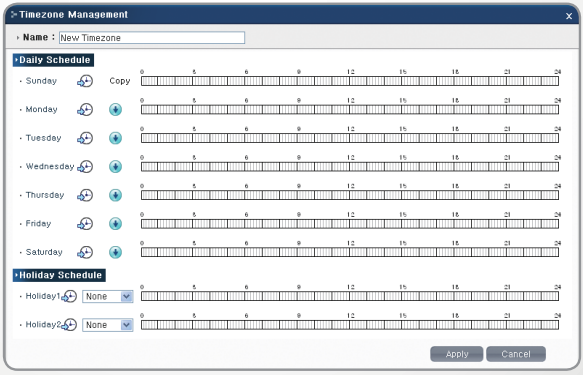
Timezone Management

- **Always** and **Never** are default time zones and cannot be deleted or modified.
- You can allow access at all times by selecting **Always**.
- You can restrict access at all time by selecting **Never**.

Adding a Time Zone

1 Click **Add**. The Timezone Management window will be displayed.

2 Enter a name for a time zone.



3 Set a time zone for each day of the week from the General Schedule.

- You can create a schedule by dragging the mouse across the timebar or manual input by clicking on the clock with an arrow pointing right.
- Each day may include as many as five distinct time periods.
- Click the arrow pointing downwards to apply the day's schedule to the following day.
- Drag the mouse across the timebar while pressing the 'Ctrl' button simultaneously, and the newly dragged parts are set as a schedule.

4 Set a time zone for each holiday schedule from the Holiday Schedule menu.
Up to two holiday schedules can be selected.

i. Select a holiday group from the holiday drop-down menu.
Each day may include as many as five distinct time periods.

ii. Drag on the mouse across the timebar or manual input by clicking on the clock with an arrow pointing right.

iii. In order to set an additional time zone for a holiday schedule, repeat steps i and ii.

5 Click **Apply** to update the time zone.
Click **Cancel** to cancel the update.

Modifying a Time Zone

1 Select a desired time zone from the list. A window for modifying a time zone is displayed.

2 Re-enter a name to change.

3 Modify a time zone for each day of the week from the schedule.

- You can modify a schedule by dragging the mouse across the timebar or manual input by clicking on the clock with an arrow pointing right.
- Each day may include as many as five distinct time periods.
- Click the arrow pointing downwards to apply the day's schedule to the following day.
- Drag the mouse across the timebar while pressing the 'Ctrl' button simultaneously, and the newly dragged parts are set as a schedule.

4 Modify a time zone for each holiday schedule from the schedule for each holiday. You can change a time zone by selecting up to two holiday schedules.

i. Select a holiday group from the holiday drop-down menu.
Each day may include as many as five distinct time periods.

ii. Drag on the mouse across the timebar or manual input by clicking on the clock with an arrow pointing right.

iii. In order to set an additional time zone for a holiday schedule, repeat steps i and ii.

5 Click **Apply** to update the timezone list.
Click **Cancel** to cancel the update.

Deleting a Time Zone

1 Check a checkbox of a desired time zone.

2 Click **Delete** to remove the selected timezones.

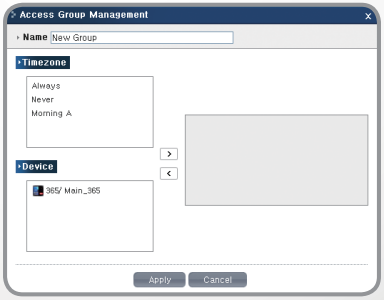
Access Group Management

- The access group tool is an advanced feature to provide schedules for each device in a group.
- The devices and timezones must be setup in order to begin access group configurations.
- **Full Access** and **No Access** are default access groups and cannot be deleted or modified.
- You can allow access on all devices at all times by selecting **Full Access**.
- You can restrict access on all devices at all time by selecting **No Access**.

Adding an Access Group

1 Click **Add**. The Access Group Management window will be displayed.

2 Enter a name for a new group.



3 Select a time zone to allow access.

4 Select a device to allow access.

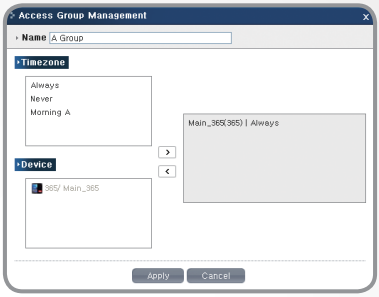
5 Click < or > to add and remove access rights from the group.

6 Click **Apply** to update the access control list.
Click **Cancel** to cancel the update.

Modifying an Access Group

1 Click a desired access group. A window for modifying an access group is displayed.

2 Modify the desired fields.



3 Click **Apply** to apply the change.
Click **Cancel** to cancel the change.

Deleting an Access Group

1 Select the checkbox of a desired access group(s).

2 Click **Delete** to delete the selected access groups.

Chapter 8

Using the System Profile Menu

Screen View

System Configuration Management

Backup System Configuration

Restore System Configuration

User Information Management

Backup User Information

Restore User Information

Language Resource Management

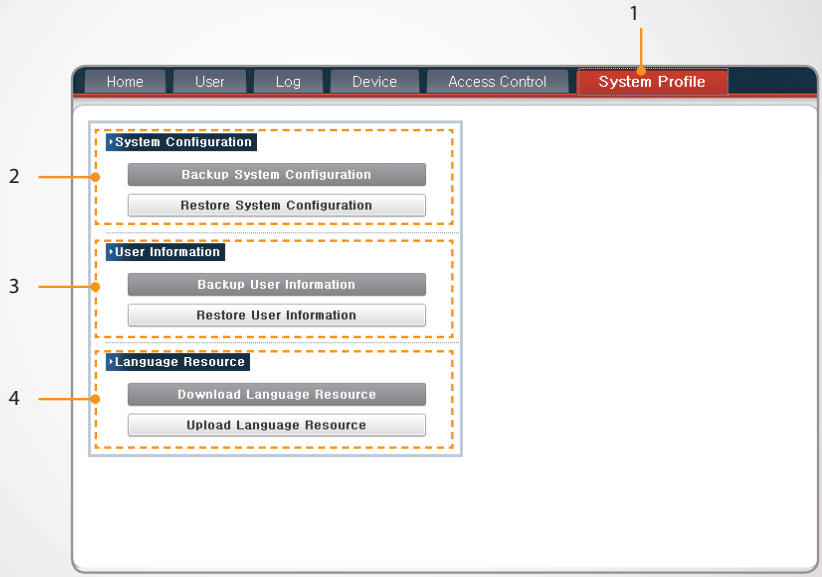
Download Language Resource

Upload Language Resource

Using the System Profile Menu

The system profile submenu is used to backup and restore various BioStar Lite server settings.

Screen View



1 **System Profile Menu Tab**: Click the tab to access the system profile menu.

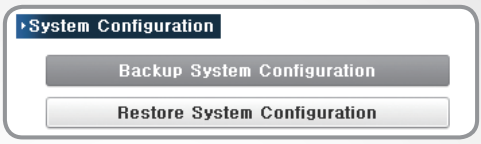
2 **System Configuration Management**: Backup or restore the device settings.

3 **User Information Management**: Backup or restore the user information.

4 **Language Resource Management**: Download or change the language resources.

System Configuration Management

The system configuration management submenus are used to backup and restore the system configuration backup file.



Backup System Configuration

1. Click **Backup System Configuration**.
2. When a pop-up window appears, click **Download** within the popup window.
3. Select a location to save the system settings backup files in.
   The device settings backup files will be saved on the designated path.

Restore System Configuration

1. Click **Restore System Configuration**.
2. Click **Browse** within the popup window.
3. Navigate and select the system configuration backup file.
4. Click **Apply** to restore the settings.

   Click **Cancel** to cancel restoration.

NOTE

- The master device may malfunction if the backup files were corrupted.
- If the system configuration backup file is not downloaded, click the right mouse button and then press 'Save as'.

User Information Management

The user information management submenus are used to backup and restore the user DB backup file.

Backup User Information

1 Click **Backup User Information** to create a backup of the User DB.

2 When a pop-up window appears, click **Download**.

3 Select a location to save the user DB backup file.
The user DB backup file will be saved on the designated path.

Restore User Information

1 Click **Restore User Information** to restore a previously backed up user DB.

2 Click **Browse** within the popup window.

3 Navigate and select the user DB backup file.

4 Click **Apply** to restore the user DB.

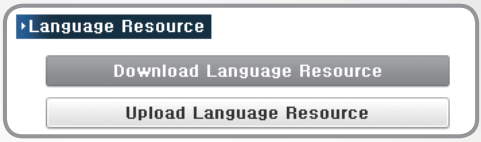
Click **Cancel** to cancel restoration.

NOTE

- The master device may malfunction if the backup files were corrupted.
- If the user DB backup file is not downloaded, click the right mouse button and then press 'Save as'.

Language Resource Management

The language resource management submenus are used to backup and restore the language table file.



Download Language Resource

1. Click **Download Language Resource** to save a language table from BioStar Lite.
2. Click a language table to restore: **English**, **Korean**, or **Custom**.
3. Select a location to save the language table.

   The language table will be saved on the designated path.

Upload Language Resource

1. Click **Upload Language Resource** to input a language table into BioStar Lite.
2. Select a language system to overwrite: **English**, **Korean**, or **Custom**.
3. Click **Browse** to select the resource file path.
4. Navigate to and select the desired language table.
5. Click **Apply** to apply the change. Click **Cancel** to cancel the change.

NOTE

- In order to change phrases for each language that are displayed on BioStar Lite, the relevant content needs to be modified on the resource files and reapplied to the device.
- When you modify resource files that are downloaded from BioStar Lite, the existing rules for writing resource files must be followed. If not, the device may malfunction.
- If the language resource backup file is not downloaded, click the right mouse button and then press 'Save as'.

Appendix

Understanding the Product Details

Introducing Devices Supporting BioStar Lite

Notes for Authenticating Fingerprints on the Device

Authentication Mode Supported by Devices

Detailed Diagram

Device Connections

Door Connections

Troubleshooting

Glossary

Index

Appendix

Understanding the Product Details

Introducing Devices Supporting BioStar Lite

BioStation T2

BioStation T2 is a device to control access and check attendance based on an IP network with a 5-inch touch screen LCD and face detection technology. It processes up to 1:3,000 authentications within one second with a built-in high-performance CPU and supports various interfaces such as WiFi, PoE, RS485, and Wiegand, while having a video phone and imbedded web server function. Also, it provides an intuitive GUI based on a touch screen and enables authentication by using an RF card and password.

X-Station

X-Station is a device to control access and check attendance with an RF card based on an innovative IP network with a touch screen LCD and face detection technology. It provides an intuitive GUI based on a 3.5-inch touch screen and enables authentication by using an RF card and password. Also, it detects faces with a built-in camera and stores a maximum of 200,000 users by utilizing 1 GB of a built-in flash memory and 256 MB of RAM.

Notes for Authenticating Fingerprints on the Device

Since it is important to scan high-quality fingerprint images when registering fingerprints, please note the details below prior to registering fingerprints.

- Check if the registrant's fingerprints are clean and dry. If needed, place a finger on the sensor again after wiping a fingerprint to be registered with a dry cloth, or blow onto a fingerprint if it is too dry.
- The same fingerprint must be scanned twice in order to register two fingerprints for the same finger. Each user can register two fingers (four fingerprints).
- Do not scan a finger with a scar or faint fingerprint.
- If the fingerprint recognition rate is low, it is recommended to delete the relevant fingerprint information and register a new fingerprint.

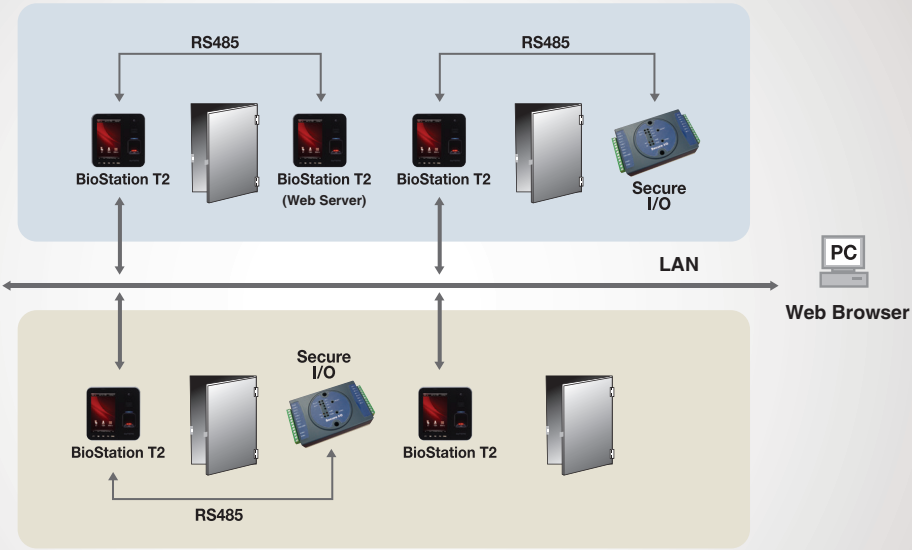
In order to obtain high-quality fingerprint information, the registrant should try to cover the entire area of the sensor with a fingerprint. Since it is better to use a finger convenient for placing onto the sensor, it is recommended to register fingerprints of an index or middle finger. The fingerprint can be properly registered by placing a finger onto the sensor and covering the surface of the sensor.

Authentication Mode Supported by Devices

	BioStation T2	BioStation	BioLite Net	BioEntry Plus	X-Station	Xpass	NOTE
Fingerprint	Fingerprint	1:N Used	1:N Used	Finger Card + Finger	X	X	
	Finger + PW	1:N Used	1:N Used	X	X	X	
	Key + Finger	1:N - OK key/ T&A key	1:N – OK key/ T&A key	X	X	X	
	Key + Finger + PW	1:N -OK key/ T&A key	1:N – OK key/ T&A key	X	X	X	
Card	Card	Card	Card	Card + Finger	Card	Card	*For BLN, if fingerprint is set for authentication, card or ID cannot be set for authentication. If you want to set both fingerprint and card for authentication, you should set the Private Authentication. *For BEPL, if only the card is set for authentication, you should set the Private Authentication.
	Card + Finger	Card/ID + Finger	Card/ ID + Finger	Card + Finger	X	Card	
	Card + PW	Card/ID + PW	Card/ID + PW	Card + Finger	Card/ID + PW	Card	
	Card + PW/Finger	Card/ ID+PW/ Finger	Card/ ID+PW/ Finger	Card + Finger	Card/ID + PW	Card	
	Card + Finger + PW	Card/ ID + Finger + PW	Card/ ID + Finger + PW	Card + Finger	Card/ID + PW	Card	
ID	ID + Finger	Card/ ID + Finger	Card/ ID + Finger	X	X	X	
	ID + PW	Card/ ID + PW	Card/ ID + PW	X	Card/ID + PW	X	
	ID + PW/ Finger	Card/ ID + PW/Finger	Card/ ID + PW/ Finger	X		X	
	ID + Finger + PW	Card/ ID + Finger + PW	Card/ ID + Finger + PW	X		X	

Detailed Diagram

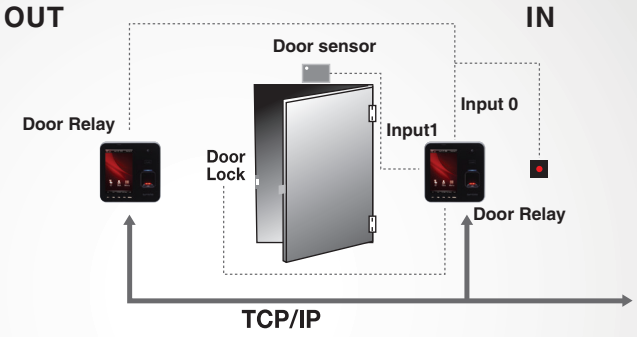
Device Connections



Door Connections

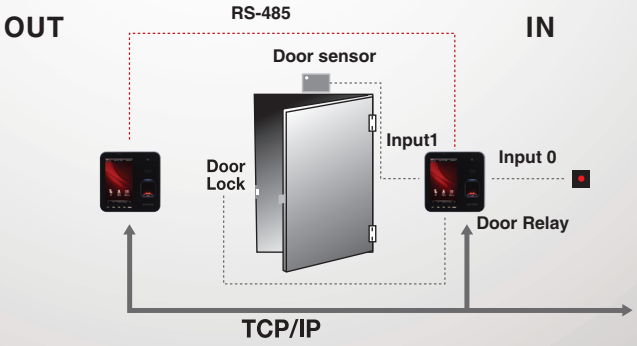
- **Standard**

  An inner device controls the door lock and is connected with an outer device by the general input trigger. (Available only when RTE is set to N/O)



- **Secure**

  An inner device controls the door lock and is connected with an outer device by the RS-485 ports (using encrypted communication with tightened security).



Troubleshooting

When any issues arise while using BioStar Lite, you can request technical support from Suprema via email (sales@supremainc.com). When you send an email, please include the following information:

- The version of BioStar Lite that you are using
- The model and firmware version of the Suprema device that you are using
- A detailed error message if an error message appears
- A brief description regarding the issue
- Your name and title

Glossary

- **Resource Files**

  Resource files refer to files in which phrases displayed on BioStar Lite are saved.

- **CSN Card Mode**

  In CSN card mode, when the card is inserted, the identification number on the card is authenticated by being compared to the identification number registered on the device. When a user is registered, the identification number assigned to the card is saved on the device.

- **APB (Anti-passback)**

  Anti-passback is a function that restricts access to each device. APB blocks the unauthorized access attempts by those who, with no previous access authentication records, try to enter using an accessible card or follow the authorized user into the office or building.

- **Distributed Processing**

  In the BioStar Lite system, the authentication database is distributed to each device. Hence, authentication is faster and can continue even when other parts of the system are offline.

- **Door**

  Doors are physical barriers that provide entry into a building or space. At least one device must be connected to a door to provide access control. However, two devices should be connected to support the anti-passback feature.

- **SSID (Service Set Indentifier)**

  SSID is a unique, 32-byte identifier on each header of packets transmitted over wireless LANs, which is used as an ID for a wireless device when connected. Since SSID distinguishes one wireless LAN from another, all APs or wireless devices to be connected to a particular wireless LAN must use the same SSID.

- **Fingerprint Authentication**

  Fingerprint Authentication is an automated process of matching two human fingerprints: the previously recorded one and the currently entered one. This product incorporates Suprema's exclusive, award-winning algorithms for recognizing fingerprints.

- **Fingerprint Sensor**

  A fingerprint sensor is an electronic device used to capture digital images of fingerprint patterns. The fingerprint captured by the fingerprint sensor is saved as raw data. These raw data are processed to create a biometric template (a collection of characteristics of an individual fingerprint) that is stored and used for user authentication.

- **Biometrics**

  Biometrics refers to a technology that utilizes a part of the human body to identify an individual. BioStar Lite incorporates Suprema's exclusive fingerprint recognition technologies, allowing access only to those who are identified biometrically.

- **FRR (FRR, False Reject Rate)**

  The false rejection rate is a probability that the system will incorrectly reject an access attempt by an authorized user. The FRR is the ratio of the number of false rejections to the number of all identification attempts.

- **Secure I/O**

  Secure I/O is an extended I/O box that performs encoded RS485 communications with devices. If the built-in I/O of a device is used, the door may be opened when the device is physically damaged. If the Secure I/O is used, the door can be prevented from being opened when the device is physically damaged.

Index

A

Adding a Holiday 56
Adding an Access Group 61
Adding a Time Zone 58
Adding Devices 17
Adding Doors 20
Administrator Account Management 25
Anti-passback 21
Authentication Mode 71

B

Backup System Configuration 65
Backup User Information 66
BioStar Lite Firmware version 24

C

Card Authentication 44
Card ID 34
CSN Mode 52
CSV Format 41

D

Deleting a Holiday 57
Deleting an Access Group 62
Deleting a Time Zone 60
Device Connections 72
Door Connections 73
Door Management 20
Download Language Resource 67
Dual Authentication 44

E

Entering General Information 33
Event Logs 37

F

Face Detection 44
Fake Detect 52
Fast Mode 52
Fingerprint Authentication 44

I

ID Authentication 44

M

Match Timeout 44
Modifying a Holiday 57
Modifying an Access Group 62
Modifying a Time Zone 59
Modifying Door information 22

N

New User Registration 32

P

Private Authentication 44

R

Registering a Card 34
Restore System Configuration 65
Restore User Information 66
RS232 47
RS485 47
RS485 Search 17

S

Scanning a Fingerprint 34
Scan Timeout 52
Searching Users 31
Search Logs 38, 39
Security Level 52
Sensitivity 53
Setting a Language 24
Setting Background 49
Setting Backlight Timeout 50
Setting Data Format 50
Setting IP Address 46
Setting Language 49
Setting Menu Timeout 50
Setting Network 45
Setting Popup Timeout 50
Setting Serial 47
Setting Show Central Clock Display 49
Setting Theme 49
Setting the Volume 50
Setting Time 49
Setting WLAN 46

T

TCP Search 17

U

UDP Search 17
Upload Language Resource 67
User Information Modification 35

V

View Image 53
Viewing Help Manual 24

Suprema Inc.

16F Parkview Tower, 6 Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Korea

Tel: +82-31-783-4502 I Fax: +82-31-783-4503

Email: sales@supremainc.com I Homepage: www.supremainc.com